APPENDIX D

Template

Privacy Impact Assessment for the Use of CCTV

By

State and Local Entities

Overview

The overview should include:

- The system or program's technical and commonly referred-to name and the organization responsible for its implementation and oversight.
- The name of the Federal, state, local, or other entities that operate, oversee, or have access to the system and program
- The objective of the program and how it relates to the governmental entity's mission
- A general description of the technology, the system, and the program.
    - Technology: for example, a description of the camera and recording technologies, with model numbers, vendors, and functions.
    - System: for example, a description of the network of surveillance devices—where and how they are installed, the number of devices, the system for collecting and, if applicable, monitoring the visual information.
    - Program: for example, a description of the law enforcement program that oversees or uses the surveillance technology – its development, funding, purpose, and limitations.

A clear and concise overview provides the reader the context in which to view the remainder of the PIA.

<< ADD Overview Here >>

Section 1.0 The System and the Information Collected and Stored Within the System

The following questions are intended to define the scope of the information collected, as well as the reasons for its collection as part of the program being developed. The term "information" includes all images and footage captured by the camera system and any information associated with those images that can be linked to individuals. If the images are viewed but not stored, please indicate that process below.

1.1 What information is to be collected?

(Please check the following if applicable)
The System's technology enables it to record:

☐ Video
    Static Range:
    Zoom Range:
    Pan from one angle to another:
☐ Tracking
    ☐ Automatic (for example, triggered by certain movements, indicators)
    ☐ Manual (controlled by a human operator)
☐ Sound
    Frequency Range:

Provide a description of what the camera is intended to view.

<<ADD Answer Here>>

The System typically records:

- ☐ Textual information (such as license plate numbers, street and business names, or text written on recorded persons' belongings).
- ☐ Images not ordinarily available to a police officer on the street:
  - ☐ Inside commercial buildings, private homes, etc.
  - ☐ Above the ground floor of buildings, private homes, etc.

☐ The System does not record or store the images.

Sample screenshots of a typical recording may be a helpful item to include in an appendix to the PIA.

1.1.1 If the activity or program seeks any specific information or types of information, please specify what is being sought.

<< ADD Answer Here>>

1.1.2 Is the information obtained from the CCTV monitoring combined with any other information; and if so, please describe the other information.

<<ADD Answer Here>>

1.2 From whom is the information collected?

- ☐ General public in the monitored areas.
- ☐ Targeted populations, areas, or activities (please describe).
- ☐ Program personnel are directed to focus on particular people, activities, or places.

1.2.1 Describe any training, guidance, or policies given to program personnel that direct them to focus on particular people, activities, or places.

<< ADD Answer Here >>

1.3 Why is the information being collected? Identify all that apply.

- ☐ For traffic-control purposes
- ☐ Crime prevention
- ☐ Crime detection
- ☐ To aid in criminal prosecution
- ☐ Threat identification
- ☐ Terrorism investigation
- ☐ Terrorism prevention
- ☐ Other (please specify)

1.3.1 Policy Rationale

Provide a brief description stating why cameras are necessary to the program and to the governmental entity's mission. Description may address one or more of the following:

- ☐ Crime prevention rationale: (For example: (1) Crimes in-progress may only be prevented if the cameras are monitored in real-time. (2) A clearly visible camera alerting the public that they are monitored may deter criminal activity, at least in the monitored area.)
- ☐ Crime investigation rationale: (For example: A hidden camera may be investigative, providing after-the-fact records of persons and locations that may be subpoenaed.)
- ☐ Terrorism rationale: (For example: Video footage is collected to compare against information contained in terrorist databases.)

1.3.2 Detail why the particular cameras, their specific placement, the exact monitoring system and its technological features were selected to advance the governmental entity's mission. For example, describe how low-light technology was selected to combat crime at night. It is not sufficient to merely state the general purpose of the system.

<< ADD Answer Here >>

1.3.3 Are you using the cameras to track and/or to identify individuals?

<<ADD Answer Here>>

1.4 How is the information collected?

- ☐ Real-time monitoring, with footage streamed, but not stored.
- ☐ Real-time monitoring with footage stored.
- ☐ Footage not monitored, only stored.

1.5 Operating Policies and Procedure

Describe the policies governing how the records can be deleted, altered or enhanced, either before or after storage. Are there access control policies limiting who can see and use the video images and for what purposes? Are there auditing mechanisms to monitor who accesses the records, and to track their uses, and if so, are these mechanisms a permanent and unalterable part of the entire system? What training was conducted for officials monitoring or accessing the technology?

<< ADD Answer Here >>

1.6 Effectiveness

Describe how the governmental entity will evaluate the camera system's performance. Are there specific metrics established for evaluation? Is there a specific timeline for evaluation?

<< ADD Answer Here >>

1.7 Cost Comparison

Has the governmental entity done a cost comparison of the camera system to alternative means of addressing the system's purposes that may have less of an impact on privacy? If so, provide a summary of such cost comparison. (For example, compare the cost of the camera system to adding law enforcement personnel to patrol the area.)

<< ADD Answer Here >>

1.8 What specific legal authorities, arrangements, and/or agreements govern the camera system?

The section should include a description of the legislative authorization at the Federal, State, and/or local level, as well as any executive or law enforcement decision authorizing the system. In addition, provide a list of the limitations or regulations controlling the use of the camera system. This may include existing law enforcement standards, such as subpoenas and warrants, or surveillance-specific rules. For example, is a warrant required for tracking or identifying an individual?

<< ADD Answer Here >>

1.9 The Decision Making Process

Describe the decision making process that led to the purchase of the camera system.

- ☐ Decision-making process included public comment or review
- ☐ Entity making the decision relied on:
  - ☐ case studies
  - ☐ research
  - ☐ hearings
  - ☐ recommendations from camera vendors
  - ☐ information from other localities
  - ☐ other (please specify)

<< ADD Answer Here >>

1.10 The Funding

- ☐ DHS Grant
- ☐ General revenues
- ☐ Law enforcement budget
- ☐ Other (please specify)
- ☐ Funding has limited duration (please specify)
- ☐ Funding renewal is contingent on program evaluation

<< ADD Answer Here >>

1.11 Privacy Impact Analysis

Given the amount and type of data collected, and the system's structure, purpose and use, discuss what privacy risks were identified and how they were mitigated. If during the system design or

technology selection process, decisions were made to limit the scope of surveillance or increase accountability, include a discussion of this decision.
Relevant privacy risks you can discuss include:

- **Privacy rights**. For example, cameras can capture individuals entering places or engaging in activities where they do not expect to be identified or tracked. Such situations may include entering a doctor's office, or an Alcoholics Anonymous, social, political, or religious meeting.
- **Freedom of speech and association**. Cameras may give the government records of what individuals say, do, and read in the public arena, for example documenting the individuals at a particular rally or associations between individuals. Such recording may chill constitutionally-protected expression and association.
- **Government accountability and procedural safeguards**. While the expectation is that law enforcement and other authorized personnel will use the technology legitimately, the program design should anticipate and safeguard against unauthorized uses, including creating a system of accountability for all uses.
- **Equal protection and discrimination**. Government surveillance, because it makes some policing activities invisible to the public, poses heightened risks of misuse, such as profiling by race, citizenship status, gender, age, socioeconomic level, sexual orientation, or otherwise. Decisions about camera placement, and dynamic decisions about camera operation, should be the product of rationale, non-discriminatory processes and inputs. System decisions should be scrutinized with fairness and non-discrimination concerns in mind.

  << ADD Answer Here >>

Section 2.0 – Uses of the System and Information

2.1 Describe uses of the footage or images derived from the cameras.

Please describe in detail how the footage or images are used, as well as how the footage or images may be used in the future.

<< ADD Answer Here >>

2.2 Privacy Impact Analysis

Describe any types of controls that are in place to ensure that the footage or images is handled in accordance with the above described uses. For example, is appropriate use of the information covered in training for all users of the system? Are audit logs regularly reviewed? What disciplinary programs are in place if an individual is found to be inappropriately using the technology or records?

<< ADD Answer Here >>

Section 3.0 – Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What is the retention period for the information in the system (i.e., how long are footage or images stored)?

- ☐ 24-72 hours
- ☐ 72 hours – 1 week
- ☐ 1 week – 1 month
- ☐ 1 month – 3 months
- ☐ 3 months – 6 months
- ☐ 6 months – 1 year
- ☐ more than 1 year (please describe)
- ☐ indefinitely

3.1.1 Describe any exemptions for the retention period (i.e. Part of an investigation or review)

<< ADD Answer Here >>

3.2 Retention Procedure

- ☐ Footage or images are automatically deleted after the retention period expires
- ☐ System operator required to initiate deletion
- ☐ Under certain circumstances, officials may override detention period:
  - ☐ To delete the footage or images before the detention period
  - ☐ To retain the footage or images after the detention period
  - ☐ Please describe the circumstances and official process for override

3.3 Privacy Impact Analysis:

Considering the purpose for retaining the information, explain why the information is maintained for the designated period.

<< ADD Answer Here >>

Section 4.0 – Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing *within* the program's operation, for example, sharing with various units or divisions within the police department in charge of the camera system. *External sharing with outside entities will be addressed in the next section.*

4.1 With what internal entities and types of personnel will the information be shared?

Internal Entities

- ☐ Investigations unit
- ☐ Auditing unit
- ☐ Financial unit
- ☐ Property-crimes unit
- ☐ Street patrols

☐ Command unit
☐ Other (please specify)
☐ None

Types of Personnel
☐ Command staff (please specify which positions)
☐ Middle management (please specify)
☐ Entry-level employees
☐ Other (please specify)

4.2 For the internal entities listed above, what is the extent of the access each receives (i.e. what records or technology is available to them, and for what purpose)?

<< ADD Answer Here >>

4.2.1 Is there a written policy governing how access is granted?

☐ Yes (please detail)
☐ No

4.2.2 Is the grant of access specifically authorized by:

☐ Statute (please specify which statute)
☐ Regulation (please specify which regulation)
☐ Other (please describe)
☐ None

4.3 How is the information shared?

4.3.1 Can personnel with access obtain the information:

☐ Off-site, from a remote server
☐ Via copies of the video distributed to those who need it
☐ Only by viewing the video on-site
☐ Other (please specify)

4.4 Privacy Impact Analysis:

Considering the extent of internal information sharing, discuss what privacy risks were identified and how they were mitigated. For example, discuss any access controls, encryption, training, regulations, or disciplinary procedures that will ensure only legitimate uses of the system within the department.

<< ADD Answer Here >>

Section 5.0 – External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to your operation – including Federal, State and Local Government, as well as private entities and individuals.

5.1 With which external entities is the information shared?

List the name(s) of the external entities with whom the footage or images and related information will be shared. The term "external entities" refers to individuals or groups outside your organization.

- ☐ Local government agencies (please specify)
- ☐ State government agencies (please specify)
- ☐ Federal government agencies (please specify)
- ☐ Private entities:
  - ☐ Businesses in monitored areas
  - ☐ Insurance companies
  - ☐ News outlets
  - ☐ Other (please specify)
- ☐ Individuals:
  - ☐ Crime victims
  - ☐ Criminal defendants
  - ☐ Civil litigants
  - ☐ General public via Public Records Act or Freedom of Information Act requests
  - ☐ Other (please specify)

5.2 What information is shared and for what purpose?

5.2.1 For each entity or individual listed above, please describe all of the following:

- ☐ The purpose for disclosure
- ☐ The rules and regulations governing disclosure
- ☐ Conditions under which information will not be disclosed
- ☐ Citations to any specific authority authorizing sharing of the camera footage or images

5.3 How is the information transmitted or disclosed to external entities?

- ☐ Discrete portions of camera footage or images are shared on a case-by-case basis
- ☐ Certain external entities have direct access to camera footage or images
- ☐ Real-time feeds of footage or images between agencies or departments
- ☐ Footage or images are transmitted wirelessly or downloaded from a server
- ☐ Footage or images are transmitted via hard copy
- ☐ Footage or images may only be accessed on-site

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with each external organization with whom information is shared, and does the MOU reflect the scope of the information currently shared?

☐ Yes
☐ No

If an MOU is not in place, explain steps taken to address this omission.

5.5 How is the shared information secured by the recipient?

For each interface with a system outside your operation:

☐ There is a written policy defining how security is to be maintained during the information sharing
☐ One person is in charge of ensuring the system remains secure during the information sharing (please specify)
☐ The external entity has the right to further disclose the information to other entities
☐ The external entity does not have the right to further disclose the information to other entities
☐ Technological protections such as blocking, face-blurring or access tracking remain intact one information is shared
☐ Technological protections do not remain intact once information is shared

5.6 Privacy Impact Analysis:

Given the external sharing, what privacy risks were identified? Describe how they were mitigated. For example, if a sharing agreement is in place, what safeguards (including training, access control or assurance of technological privacy protection) have been implemented to ensure information is used appropriately by agents outside your department/agency?

<< ADD Answer Here >>

Section 6. 0 – Technical Access and Security

6.1 Who will be able to delete, alter or enhance records either before or after storage?

☐ Command staff
☐ Shift commanders
☐ Patrol officers
☐ Persons outside the organization who will have routine or ongoing access to the system (please specify)
☐ Other (please specify)

6.1.1 Are different levels of access granted according to the position of the user? If so, please describe.

- ☐ All authorized users have access to real-time footage or images
- ☐ Only certain authorized users have access to real-time footage or images (please specify which users)
- ☐ All authorized users have access to stored footage or images
- ☐ Only certain users have access to stored footage or images (please specify which users)
- ☐ All authorized users can control the camera functions (pan, tilt, zoom)
- ☐ Only certain authorized users can control the camera functions
- ☐ All authorized users can delete or modify footage or images
- ☐ Only certain authorized users can delete or modify footage or images (please specify which users)

6.1.2 Are there written procedures for granting access to users for the first time?

- ☐ Yes (please specify)
- ☐ No

6.1.3 When access is granted:

- ☐ There are ways to limit access to the relevant records or technology (please specify)
- ☐ There are no ways to limit access

6.1.4 Are there auditing mechanisms:

- ☐ To monitor who accesses the records?
- ☐ To track their uses?

6.1.5 Training received by prospective users includes discussion of:

- ☐ Liability issues
- ☐ Privacy issues
- ☐ Technical aspects of the system
- ☐ Limits on system uses
- ☐ Disciplinary procedures
- ☐ Other (specify)
- ☐ No training

The training lasts:

- ☐ None
- ☐ 0-1 hours
- ☐ 1-5 hours
- ☐ 5-10 hours
- ☐ 10-40 hours

☐ 40-80 hours
☐ More than 80 hours

The training consists of:
☐ A course
☐ A video
☐ Written materials
☐ Written materials, but no verbal instruction
☐ None
☐ Other (please specify)

6.2 The system is audited:

☐ When an employee with access leaves the organization
☐ If an employee is disciplined for improper use of the system
☐ Once a week
☐ Once a month
☐ Once a year
☐ Never
☐ When called for

6.2.1 System auditing is:

☐ Performed by someone within the organization
☐ Performed by someone outside the organization
☐ Overseen by an outside body (for example a city council or other elected body – please specify)

6.3 Privacy Impact Analysis:

Given the sensitivity and scope of information collected, what privacy risks related to security were identified and mitigated?

<< ADD Answer Here >>

Section 7.0 – Notice

7.1 Is notice provided to potential subjects of camera recording that they are within view of a camera?

☐ Signs posted in public areas inform the public of recording by cameras
☐ Signs in multiple languages
☐ Attached is a copy of the wording of such notice signs
☐ Notice is not provided
☐ Other (please describe)

Section 8.0 – Technology

The following questions are directed at analyzing the selection process for any technologies used by the camera system, including cameras, lenses, and recording and storage equipment.

8.1 Were competing technologies evaluated to compare their ability to achieve system goals, including privacy protection?

☐ Yes
☐ No

8.2 What design choices were made to enhance privacy?

☐ The system includes face-blurring technology
☐ The system includes blocking technology
☐ The system limited location to address privacy
☐ The system has other privacy-enhancing technology (Please specify)
☐ None (Please specify)

Section 9.0 – Attachments to the PIA

☐ Authorizing legislation
☐ Grant documents
☐ Transcript of public hearing or legislative session
☐ Press release announcing the CCTV program
☐ Program manuals outlining the system's rules and regulations
☐ Other (please specify)

Responsible Officials

<< ADD Project Manager>>

APPENDIX D

Civil Liberties Impact Assessment
for the

DATE

Contact Point

Reviewing Official

Officer for Civil Rights and Civil Liberties

(202) XXX- XXXX

Introduction

[Include a summary of the program being reviewed. Include a statement of the statutory and/or regulatory authority for this program.]

Potential Civil Liberties Impacts

Impact on Particular Groups or Individuals

1. *Is the program intended to have a direct impact on certain racial or ethnic groups? Even if it is not, might the program have an effect on certain racial or ethnic groups that might reasonably be perceived to be intentional?* If a program singles out one or more racial, ethnic, or national origin groups, *or is intended to do so*, the program must satisfy stringent Constitutional requirements. *See Loving v. Virginia*, 388 U.S. 1 (1967) (strict scrutiny standard of review applies where government action classifies individuals on the basis of race). If the program indirectly or unintentionally impacts upon minorities, the Constitutional standards for evaluating it are much less stringent, *requiring only a lawful, rational basis for the program, but the impact on minorities* should still be considered. *See Washington v. Davis*, 426 U.S. 299 (1976) (applying a rational basis standard of review to government regulation with disparate impact on minorities); *see also Pers. Adminr. v. Feeney*, 442 U.S. 256 (1979) (intentional discrimination, not merely discriminatory effect, is required to trigger heightened review).

2. *Would the program further the Constitutional principle of race-neutral government action, or would it encourage or depend upon a government official categorizing people by race?* Generally, an agency creating a program that singles out one or more racial or ethnic groups must show that it has narrowly tailored its program to further a compelling government interest. When the government treats certain categories of people differently than other categories, it generally must do so according to categories other than race or ethnicity (such as geography or socioeconomic status). *See, e.g., Adarand Const., Inc. v. Pena*, 515 U.S. 200, 235 (1995); *Bolling v. Sharpe*, 347 U.S. 497 (1954).

3. *How would the program affect people with disabilities?* Certain regulatory programs may work a greater hardship on persons with disabilities. If this possibility is anticipated with respect to a particular regulation, we should ask whether this aspect of the proposed rule is justified and whether the hardship can be ameliorated in the implementation of the rule. *Cf.* Rehabilitation Act of 1973, 29 U.S.C. § 794 (prohibiting discrimination on the basis of disability in programs conducted by federal agencies).

4. *How would the program affect those attempting to exercise a particular religion?* Programs identifying particular religious beliefs must be assessed strictly under the First Amendment. Generally-applicable rules that do not refer to any particular religion, but which may have an adverse effect on religious adherents'

exercise of their religion, will be assessed under a less onerous constitutional test, *see Employment Division, Dept. of Human Resources v. Smith*, 494 U.S. 872 (1990), but federal statutes may require a heightened justification for even generally-applicable rules. *See O'Bryan v. Bureau of Prisons*, 349 F.3d 399 (7th Cir. 2003) (discussing applicability of the Religious Freedom Restoration Act , 42 U.S.C. § 2000bb-1, to internal operations of the federal government). *Cf.* Religious Land Use and Institutionalized Persons Act of 2000, 42 U.S.C. § 2000cc *et seq*. (providing protection for the exercise of religion by institutionalized persons). Agencies should consider whether their programs affect the exercise of religion and whether the agency could make reasonable accommodations to avoid a negative effect.

5. *How would the program affect people with limited English language proficiency?* Title VI of the Civil Rights Act of 1964 prohibits discrimination based on national origin by recipients of federal funds. Department of Justice regulations interpret this to mean that these recipients must take reasonable steps to provide persons with limited English proficiency meaningful access to programs and services. Executive Order No. 13,166 requires the executive agencies of the federal government to meet the same standard in their own programs.

Influence of Government

6. *Would the program increase the authority, control, or influence of the federal government in its relationship with private citizens?* Specifically:

   A. *Would the program require or authorize the federal government to collect more information about private citizens?* The collection of data on law-abiding citizens reduces their control over personal information and thereby reduces their liberty. The agency should consider whether it has a sound basis for concluding that collection of the additional information is necessary to effectively carry out an important agency function. If the agency expects that obtaining the information will be beneficial, but cannot foresee with certainty whether the expected benefits will materialize, the agency could consider adding sunset provisions or provisions that commit the agency to a periodic reassessment of the benefits associated with the information collection.

   B. *Would the program require or authorize the federal government to centralize the collection of information that was previously dispersed?* While federal, state, and local government agencies collect a great deal of information on American citizens, limited permanent residents, and non-U.S. citizens, it is currently dispersed in many places, both in paper records and in databases. While it is important in many circumstances for the Department to organize the collection of data, it is also important to recognize that the federal government's centralization of information is generally met with public suspicion even when the centralized collection of information meets all legal requirements (e,g., CAPPS II and Total

Information Awareness). Centralizing information into organized government databases also increases the risk that the information collected will be used for a purpose other than that for which it was collected (commonly referred to as, "mission creep"). It also compounds the risk that compilations of information could be accessed by unauthorized persons. For these reasons, regulatory analysis of such programs should include a discussion of the civil liberties impact of centralization as opposed to a decentralized, federated or distributed approach to data collection. *See United States Dept. of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 764 (1989) ("Plainly there is a vast difference [in terms of personal privacy] between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information.").

7. *Would the program increase the authority, control, or influence of the federal government in its relationship with state or local governments?* The Constitution creates a delicate balance between federal and state governments, which helps to prevent the accumulation of excessive power in either the States or our National Government. These structural constraints on government protect our civil liberties. *See Atascadero State Hosp. v. Scanlon*, 473 U.S. 234, 242 (1985) ("The constitutionally mandated balance of power between the States and the Federal Government was adopted by the Framers to ensure the protection of our fundamental liberties.") (quotation marks and citation omitted); *Garcia v. San Antonio Metro. Transit Auth.*, 469 U.S. 528, 572 (1985) (Powell, J., dissenting) ("The Framers believed that the separate sphere of sovereignty reserved to the States would ensure that the States would serve as an effective 'counterpoise' to the power of the Federal Government."). When authority is dispersed between the various levels of government, it is less likely that a single agency can accumulate unhealthy power over our individual lives. *See also* Exec. Order No. 13,132 (1999) ("The people of the States created the national government and delegated to it enumerated governmental powers. All other sovereign powers, save those expressly prohibited the States by the Constitution, are reserved to the States or to the people.").

8. *Would the program increase the authority, control, or influence of the federal government in its relationship with the private sector?* A robust private sector also serves as a check to the authority of the government. Associations of individuals in the private sector allow for the free flow of ideas and programs that can advance the interests of individuals. The gradual layering of regulations stifles this creativity. *See* 2 Alexis de Tocqueville, *Democracy in America* 319 (Phillips Bradley ed., Vintage Books 1990) (1840) (describing what a despotic government would look like in a democratic society, and stating that such a government would "cover[] the surface of society with a network of small complicated rules, minute and uniform, through which the most original minds and the most energetic characters cannot penetrate, to rise above the crowd. . . . Such a power does not destroy, but it prevents existence; it does not tyrannize, but

it compresses, enervates, extinguishes, and stupefies a people, till [the] nation is reduced to nothing better than a flock of timid and industrious animals, of which the government is the shepherd").

9. *Would the program require or authorize the federal government to share information about private citizens with third parties outside the federal government?* If so, the legal authorities permitting the information to be shared need to be identified.

10. *Does the program include an intelligence or surveillance component? Will the program be governed by the provisions of Executive Order 12333 and/or the National Security Act of 1947?*

Notice and Redress

11. *Does the public receive notice of the program, and have the ability to file comments on it?*

12. *Are procedures available for redress of alleged violations of civil rights and civil liberties? If so, how will the public be informed of these redress procedures? Do the redress procedures provide for data corrections to be sent to all entities with which the information has been shared?*

Alternatives

13. *Is the program the least burdensome alternative with respect to civil liberties? Could the agency formulate other alternatives to accomplish the same goal while minimizing the impacts on civil liberties?* Executive Order No. 12,866 (1993), amended by Exec. Order No. 13,258 (2002), requires agencies to identify and assess alternative forms of regulation.

14. *Could the agency alter the proposed regulatory plan to enhance civil liberties?* This may involve removing established regulatory burdens when those burdens have not produced significant benefits. For example, if an agency seeks to improve security by employing a new surveillance technique where a different surveillance technique is currently in place, the agency should consider discontinuing the first surveillance technique rather than simply adding the new to the old.

15. *Will any impositions on liberty created by the program be voluntarily incurred?*

16. *Is any imposition on civil rights and civil liberties equally distributed, randomly distributed, or focused on identifiable groups?*

17. *Is any imposition on civil rights and civil liberties brief or extended?*

Safeguards

18. *Would effective implementation of the program be dependent, in whole or in part, on government employees having a heightened awareness of Constitutional rights, federal laws or regulations, or Departmental policies as they carry out their duties?* If so, the promulgating agency should consider the need to increase or strengthen training with regard to the protection of civil rights and civil liberties.

19. *Would the program increase or decrease the discretion of those employees or agents implementing the regulation?* It is possible that an increase in discretionary authority could provide the means for obscuring improper enforcement motives at times. On the other hand, additional discretionary authority may allow for special consideration in some circumstances to ease the regulatory burden on disadvantaged individuals or groups.

20. *Does the program have embedded legal counsel or ready access to legal counsel?* The active involvement of the Office of General Counsel will assist programs to avoid violations of law.

21. *Are reports to Congress, or Congressionally-mandated audits, required, and if so are they one-time or periodic in nature?* Congressional oversight provides another level of oversight for a program.

Other Rights

22. *Could the program limit protected political or religious expression? Could the program implicitly chill open discourse or a person's ability to express their beliefs in writing that does not threaten or amount to shouting fire in a theater?* There are numerous other civil liberties recognized in our founding documents and supported by legislation, regulations, court decisions and policy. While these may be less likely to placed in jeopardy by DHS programs, they nonetheless deserve mention here and should not escape the attention of program leadership. The interpretation of rights inherent in the First Amendment, such as free speech, freedom of the press, right to assemble, and the right to petition, is mostly settled. Yet, in the realm of security policy, the application of these rights requires careful scrutiny.

23. *Could the program lead to some restriction on property ownership, such as real, personal or intellectual property, firearms, or would it grant an unfair advantage to a particular business entity? Will the program have an impact on voting rights? Does the program take the least restrictive approach possible to regulating travel, including the travel of United States citizens? Does the program take away a freedom without affording proper due process?* Other liberties that a program should be evaluated against include: the right to keep and bear arms, due process rights, private property rights, rights of the accused, voting rights, the right to travel, and the presumption of innocence.

Conclusion

Responsible Officials_____, _____

Program Manager:

Approval Signature Page

_____

Officer for Civil Rights and Civil Liberties
Department of Homeland Security